网络扫描概述

通过主动发送相关的数据包进行网络探测、识别、分析分会的信息、用以确认网络目标相关的特征。
网络扫描也是信息搜集的一部分，主动探测收集目标信息，为后续漏洞的分析和利用做准备。

网络扫描类型	网络扫描目的
主机扫描	找出网段内活跃主机
端口扫描	找出主机上所开放的网络服务
操作系统/ 网络服务辨识	识别主机安装的操作系统类型与开放网络服务类型，以选择不同渗透攻击代码及配置
漏洞扫描	找出主机/网络服务上所存在的安全漏洞，作为破解通道

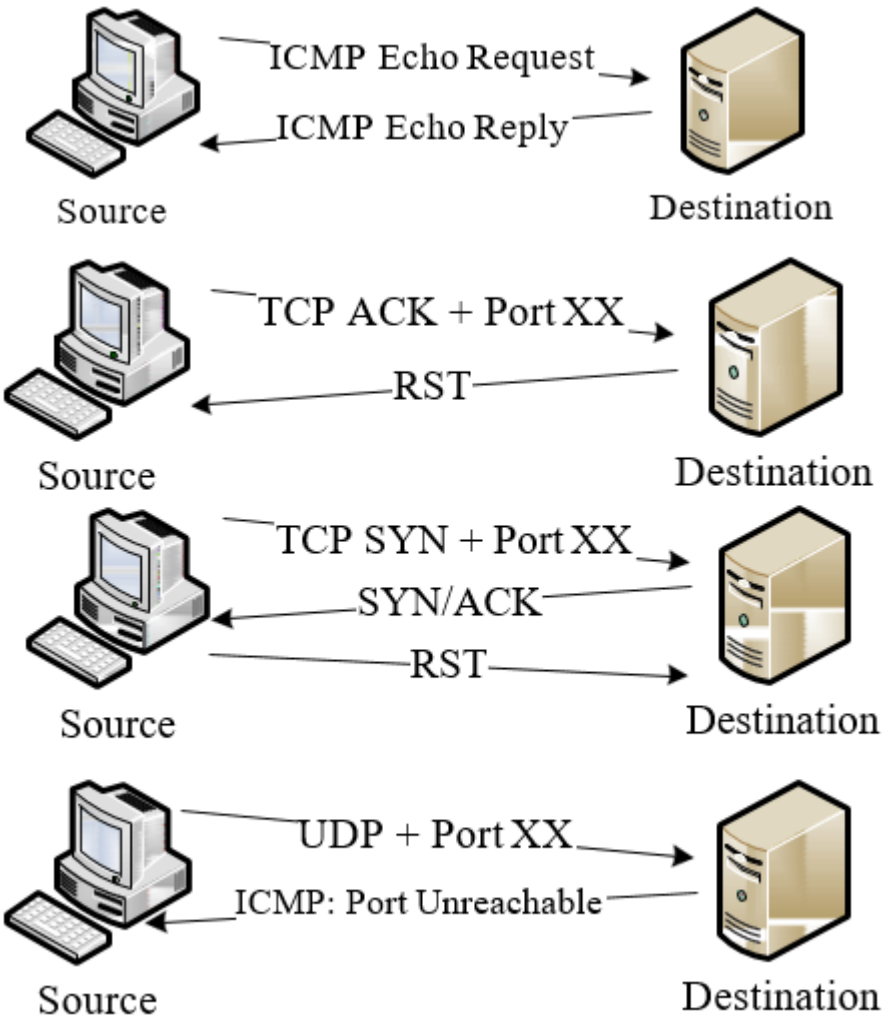
主机扫描目的：检查目标主机是否活跃
端口扫描：寻找主机在线开放的宽口，并在端口上所运行的服务，甚至可以进一步确定目标的操作系统类型和更详细的信息
系统扫描：识别主机安装的操作系统类型与开放的网络服务类型
漏洞扫描：找出主机/网络服务上所存在的安全漏洞，作为破解通道

主机扫描原理

主机扫描目的：检查目标主机是否活跃(active)

扫描方式

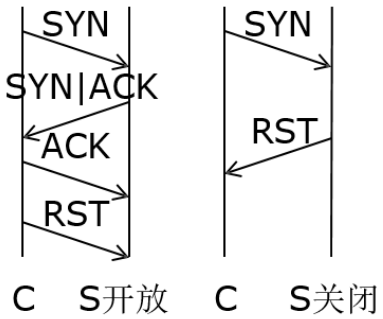
- 传统ICMP Ping扫描
- TCP扫描
- ACK Ping扫描
- SYN Ping扫描
- UDP Ping扫描


ICMP Echo Request
ICMP Echo Reply
Source
Destination
TCP ACK + Port XX
RST
Source
Destination
TCP SYN + Port XX
SYN/ACK
RST
Source
Destination
UDP + Port XX
ICMP: Port Unreachable
Source
Destination

端口扫描原理

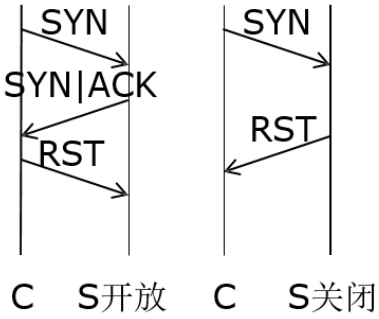
TCP连接扫描

- 调用**connect() socket**函数连接目标端口
- 开放端口：完成完整的**TCP**三次握手**(SYN, SYN|ACK, ACK)**，**timeout/RST**
- 关闭端口：**SYN, RST**
- 优势**&**弱势：无需特权用户权限可发起，目标主机记录大量连接和错误信息，容易检测



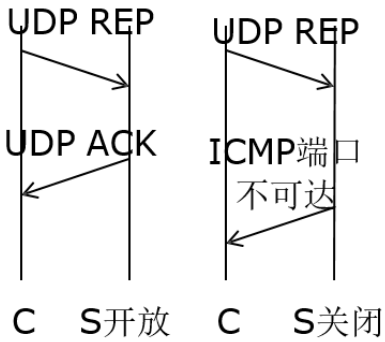
SYN扫描

- 半开扫描**(half-open scanning)**
- 开放端口：攻击者**SYN,** 目标主机**SYN|ACK,** 攻击者立即反馈**RST**包关闭连接
- 关闭端口：攻击者**SYN,** 目标主机**RST**
- 优势**&**弱势：目标主机不会记录未建立连接，较为隐蔽，需根用户权限构建定制**SYN**包



UDP端口扫描

- 对目标端口发送特殊定制的**UDP**数据报文
- 开放端口**: UDP**反馈
- 关闭端口**: ICMP port unreachable**报文



操作系统扫描

操作系统类型探查(OS Identification)

- 通过各种不同操作系统类型和版本实现机制上的差异
- 通过特定方法以确定目标主机所安装的操作系统类型和版本的 技术手段
- 明确操作系统类型和版本是进一步进行安全漏洞发现和渗透攻击的必要前提

不同操作系统类型和版本的差异性

- 协议栈实现差异－协议栈指纹鉴别
- 开放端口的差异－端口扫描
- 应用服务的差异－旗标攫取

辨识方式

- 主动－操作系统主动探测技术
- 被动－被动操作系统识别技术

网络服务扫描

网络服务类型探查

- 确定目标网络中开放端口上绑定的网络应用服务类型和版本
- 了解目标系统更丰富信息，可支持进一步的操作系统辨识和漏洞识别

漏洞扫描原理

在前面的步骤中：扫到了操作系统的版本 用漏洞代码去试探

扫到的软件版本 用漏洞代码去试探

漏洞扫描技术

- 检查系统是否存在已公布安全漏洞，从而易于遭受网络攻击的 技术。
- 双刃剑
  - 网络管理员用来检查系统安全性，渗透测试团队**(Red Team)**用于安全评估。
  - 攻击者用来列出最可能成功的攻击方法，提高攻击效率。

已发布安全漏洞数据库

- 业界标准漏洞命名库**CVE** http://cve.mitre.org
- 微软安全漏洞公告**MSxx-xxx**
  http://www.microsoft.com/china/technet/security/current.mspx
- **SecurityFocus BID**
  http://www.securityfocus.com/bid
- **National Vulnerability Database: NVD**
  http://nvd.nist.gov/

Nmap

```
Nmap被誉为"扫描器之王"，Nmap是一个开源工具，提供跨平台（Windows、linux、mac os）

功能
1．查看主机存活
2．扫描目标主机开放端口
3．识别目标主机操作系统
4．查看目标主机服务的版本信息
5．漏洞探测


运行方式：命令行、图形化工具
```

Nmap安装

网址：http://nmap.org

Nmap参数

参数分类

1. 目标说明
2. 主机发现
3. 端口扫描
4. 端口说明和扫描顺序
5. 服务与版本探测
6. 脚本扫描
7. 操作系统探测
8. 时间和新能
9. 防火墙/IDS规避和欺骗
10. 输出选项

目标说明

> TARGET SPECIFICATION

- -iL：　　从列表中输入 从主机地址列表中导入扫描地址 可以从主机的文件中导入扫描列表
- -iR：　　随机选择目标，hostnum表示目标数目，0意味着永无休止的扫描

- --exclude　　排除主机/网络
- --excludefile　　排除文件中的列表

主机发现

> HOST DISCOVERY

- -sL 扫描列表，仅将指定的目标IP列举出来，不进行主机发现
- -sn 跟-sP 一样，只利用ping扫描进行主机发现，不扫描目标主机的端口，只扫描是否在线 不扫描端口
- -Pn 将所有指定的主机视为已开启状态，跳过主机发现过程
- -PS [portlist]：TCP SYN Ping，发送一个设置了SYN标志位的空TCP报文
- -PE; -PP; -PM：ICMP Ping Types，发送ICMP Type 8 （回声请求）报文，期待从运行的主机得到一个type 0 （回声相应）报文
- n：不用域名解析，加快扫描速度
- -R：为所有目标IP地址作反向域名解析
- --system-dns：使用系统域名解析器，一般不使用该选项，因为比较慢

端口扫描

```
SCAN TECHNIQUES
```

Nmap将目标主机端口分成6种状态：

- open（开放）
- closed（关闭）
- filtered(被过滤的)
- unfiltered(未被过滤) 可访问但不确定开放情况
- open|filtered(开放或被过滤)无法确定端口是开放的还是被过滤的
- closed|filtered(关闭或被过滤)无法确认端口是关闭的还是被过滤的

Nmap产生结果是基于机器的响应报文，而这些主机可能是不可信任的，会产生一些迷惑或者误导Nmap的报文

常用命令

- -sS TCP SYN扫描，半开放状态，扫描速度快隐蔽性好（不完成TCP连接），能够明确区分端口状态
- -sT TCP连接扫描，容易产生记录，效率低
- -sA TCP ACK扫描 只设置ACK标志位，区别被过滤与未被过滤
- -sU UDP服务扫描
- –sO：IP协议扫描，可以确定目标机支持哪些IP协议（TCP, ICMP, IGMP）

端口说明和扫描顺序

> PORT SPECIFICATION AND SCAN ORDER

- –p： 只扫描指定的端口，单个端口和用连字符表示的端口范围都可以；当既扫描TCP端口又扫描UDP端口时，您可以通过在端口号前加上T: 或者U:指定协议。协议限定符一直有效您直到指定另一个。例如，参数 -p U:53，111，137，T:21-25，80，139，8080 将扫描UDP 端口53，111，和137，同时扫描列出的TCP端口。注意，要既扫描 UDP又扫描TCP，您必须指定 -sU ，以及至少一个TCP扫描类型(如 -sS，-sF，或者 -sT)
- –p： 扫描指定的端口名称，如nmap–p smtp,http 10.10.1.44
- –p U:[UDP ports],T:[TCP ports]：对指定的端口进行指定协议的扫描
- –F：快速扫描（仅扫描100个最常用的端口），nmap-services文件指定想要扫描的端口；可以用—datadir选项指定自己的小小nmap-services文件
- –top-ports： 扫描前number个端口
- –r：不要按随机顺序扫描端口，默认情况下按随机（常用的端口前移）

服务与版本探测

> SERVICE/VERSION DETECTION

nmap-services是一个包含服务的数据库，Nmap通过查询该数据库可以报告那些端口可能对应于什么服务器，但不一定正确。在用某种扫描方法发现TCP/UDP端口后，版本探测会询问这些端口，确定到底什么服务正在运行；nmap-service-probes数据库包含查询不同服务的探测报文和解析识别响应的匹配表达式；当Nmap从某个服务收到响应，但不能在数据库中找到匹配时，就打印出一个fingerprint和一个URL给您提交。 参数含义：

- –sV：打开版本探测
- –allports：不为版本探测排除任何端口，默认情况下跳过9100端口
- –version-intensity：设置版本扫描强度，范围为0-9，默认是7，强度越高，时间越长，服务越可能被正确识别
- –version-light：是—version-intensity2的别名
- –version-all：是—version-intensity9的别名
- –version-trace：跟踪版本扫描活动，打印出详细的关于正在进行的扫描的调试信息
- –sR：RPC扫描，对所有被发现开放的TCP/UDP端口执行SunRPC程序NULL命令，来试图 确定它们是否RPC端口，如果是， 是什么程序和版本号

脚本扫描

> SCRIPT SCAN

操作系统探测

> OS DETECTION

```
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
```

- –O：启用操作系统检测；-A可以同时启用操作系统检测和版本检测

- –osscan-limit：针对指定的目标进行操作系统检测
- –osscan-guess|--fuzzy：当Nmap无法确定所检测的操作系统时，会尽可能地提供最相近的匹配

时间和性能

> TIMING AND PERFORMANCE

- –min-hostgroup ;--max-hostgroup： 调整并行扫描组的大小，用于保持组的大小在一个指定的范围之内；Nmap具有并行扫描多主机端口或版本的能力，Nmap将多个目标IP地址空间分成组，然后在同一时间对一个组进行扫描。通常，大的组更有效。缺点是只有当整个组扫描结束后才会提供主机的扫描结果
- –min-parallelism; --max-parallelism： 调整探测报文的并行度，用于控制主机组的探测报文数量；默认状态下， Nmap基于网络性能计算一个理想的并行度，这个值经常改变

防火墙/IDS规避和欺骗

> FIREWALL/IDS EVASION AND SPOOFING

- –f（报文分段）; --mtu（使用指定的MTU）： 将TCP头分段在几个包中，使得包过滤器、 IDS以及其它工具的检测更加困难
- –D： 使用诱饵隐蔽扫描；使用逗号分隔每个诱饵主机，也可用自己的真实IP作为诱饵，这时可使用 ME选项说明。如果在第6个位置或更后的位置使用ME选项，一些常用端口扫描检测器(如Solar Designer's excellent scanlogd)就不会报告 这个真实IP。如果不使用ME选项，Nmap 将真实IP放在一个随机的位置
- –S <IP_Address>：源地址哄骗，说明所需发送包的接口IP地址
- –e： 使用指定的接口
- –source-port; -g： 源端口哄骗；很多产品本身会有这类 不安全的隐患，甚至是微软的产品。Windows 2000和Windows XP中包含的IPsec过滤器也包含了一些隐含规则，允许所有来自88端口(Kerberos)的TCP和UDP数据流。另一个常见的例子是Zone Alarm个人防火墙到2.1.25版本仍然允许源端口53(DNS)或 67(DHCP)的UDP包进入。
- –data-length： 发送报文时附加随机数据
- –ttl： 设置IPtime-to-live域
- –randomize-hosts：对目标主机的顺序随机排列

输出选项

> OUTPUT

- –oN： 标准输出
- –oX： XML输出写入指定的文件
- –oS： 脚本小子输出，类似于交互工具输出
- –oG： Grep输出

- –oA ： 输出至所有格式
- –v：提高输出信息的详细度
- –d [level]：提高或设置调试级别，9最高
- –packet-trace：跟踪发送和接收的报文
- –iflist：输出检测到的接口列表和系统路由
- –append-output：表示在输出文件中添加，而不是覆盖原文件
- –resume ： 继续中断的扫描，
- –stylesheet ： 设置XSL样式表，转换XML输出；Web浏览器中打开Nmap的XML输出时，将会在文件系统中寻找nmap.xsl文件，并使用它输出结果
- –no-stylesheet：忽略XML生命的XSL样式表

使用示例

```
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
```

扫描技巧示例

常用扫描方法

- nmap ip
- nmap 域名
- nmap 多个ip
- nmap ip/网段
- nmap ip范围如192.168.0.1-200
- nmap -iL test.txt 扫描某个目录里的地址
- nmap -sn或-sP **只进行主机发现**
- nmap -p80,21,8080 ip nmap -p50-800 ip **只扫描特定端口**
- nmap -vv ip 简单扫描，详细输出返回结果
- namp -traceroute 域名 简单扫描并进行路由跟踪
- nmap -O ip **探测操作系统类型**
- nmap -sS ip 扫描半开放TCP端口
- nmap -sU ip 扫描UDP 服务端口
- namp -sV ip **版本扫描**
- nmap -A ip **综合扫描** 包含1-10000端口的ping扫描，操作系统扫描，路由跟踪，服务探测

Zenmap

```
nmap -T4 -A -v   ip
-T  设置速度等级 1-5级，数字越大，速度越快
-A  综合扫描
-v  输出扫描过程
```